

Manuel d'utilisation de Blockulicious

Ce manuel vous permet de vous ***expliquer la manière*** dont vous allez pouvoir utiliser l'extension Blockulicious pour votre navigateur. Il s'agit d'un manuel complet et permettant de s'approprier le produit.

Ce manuel est pour toutes les versions et navigateurs confondus.

Comment installer Blockulicious ?

CRDF France détecte automatiquement votre configuration et votre navigateur qui est supporté par une version stable de Blockulicious. Pour installer la dernière version, merci de vous rendre sur la fiche du produit :

- En français : [Fiche produit](#)
- En anglais : [Fiche produit](#)

Présentation de Blockulicious

Blockulicious est une extension pour les navigateurs Chrome, Internet Explorer et Firefox capable de bloquer les sites internet comportant des risques pour votre ordinateur et votre vie privée. En effet, bon nombre de sites web (licites et illicites) librement accessibles sur l'Internet proposent des contenus malicieux, inappropriés, prohibés ou nuisibles à la productivité. L'accès à des sites malicieux peut avoir comme conséquence l'installation de codes malicieux à l'insu de utilisateur.

Blockulicious est un service gratuit qui vérifie chaque adresse visitée sur votre navigateur en interdisant l'accès aux sites internet réputés pour être malveillants. De plus, Blockulicious bloque même les logiciels malveillants se connectant à votre insu aux sites internet nuisibles. Ainsi, le logiciel malveillant devient inefficace sur votre ordinateur puisqu'il n'est pas capable de communiquer à travers le réseau Internet et/ou votre navigateur.

Contrairement à d'autres produits, Blockulicious protège contre les risques sécuritaires liés aux Adwares (PUP, en français logiciels non désirés) qui s'installent automatiquement sur votre ordinateur à votre insu. Blockulicious bloque également les sites internet réputés avant la plupart des produits présents sur le marché. Testez Blockulicious et adoptez le dès maintenant !

Ce produit a été développé conjointement avec [CRDF Labs](#) et [ADMINUSLabs](#). Ce logiciel utilise les bases de données de CRDF Labs et ADMINUSLabs. Un gage qualité dans le monde de la sécurité informatique puisque nous fournissons la plupart des produits du marché en bases de données contenant les sites internet malveillants réputés.

Navigateurs supportés

Blockulicious supporte actuellement en version stable les navigateurs suivants :

- Google Chrome ou Chromium
- Mozilla Firefox (version beta actuellement)

Types de menaces bloquées par Blockulicious

Pour garantir une efficacité optimale, CRDF Labs insère des nouvelles entrées dans sa base de données toutes les minutes. Nous avons une philosophie particulière et différente des autres produits de protection (qui font la même chose que Blockulicious). Nous bloquons les catégories de sites internet comprenant ces risques :

- Les sites malveillants contenant des logiciels malicieux (virus, malware, adware, ...)
- Les attaques par hameçonnage (phishing)
- Les sites internet dangereux pour votre vie privée
- Les exploits (failles dans un logiciel permettant d'insérer un code malveillant capable d'infecter votre ordinateur)
- Malvertising (= les publicités légitimes pouvant être malicieuses)
- Publicités (uniquement si vous le souhaitez)

Quelques définitions importantes

Les définitions des catégories bloquées par le produit Blockulicious.

Qu'est-ce qu'un logiciel malveillant ?

Un logiciel malveillant (en anglais, malware) est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur infecté. De nos jours, le terme virus est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants. En effet, les malwares englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces. La catégorie des virus informatiques, qui a longtemps été la plus répandue, a cédé sa place aux chevaux de Troie en 2005.

Les programmes malveillants ont été développés pour de nombreux systèmes d'exploitation et applications. Pourtant, certains d'entre eux n'ont jamais été concernés. En effet, les auteurs de virus privilégient les systèmes d'exploitation largement utilisés ; les systèmes comportant des vulnérabilités ; et ceux pour lesquels une documentation détaillée est disponible (puisqu'elle inclut des descriptions des services et des règles en vigueur pour écrire des programmes compatibles). Le volume de logiciels malveillants destinés à Windows et Linux est à peu près proportionnel à leurs parts de marché respectives.

Qu'est-ce que le phishing ?

L'hameçonnage ou phishing (parfois appelé filoutage) est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale. Elle peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques.

Qu'est-ce qu'un exploit ?

Un exploit est, dans le domaine de la sécurité informatique, un élément de programme permettant à un individu ou un logiciel malveillant d'exploiter une faille de sécurité informatique dans un système d'exploitation ou dans un logiciel que ce soit à distance, remote exploit, ou sur la machine sur laquelle cet exploit est exécuté, local exploit ; ceci, afin de prendre le contrôle d'un ordinateur ou d'un réseau, de permettre une augmentation de privilège d'un logiciel ou d'un utilisateur, ou d'effectuer une attaque par déni de service.

Qu'est-ce qu'un Adware ?

Un logiciel publicitaire ou publiciel (adware en anglais) est un logiciel qui affiche de la publicité lors de son utilisation. Logiciels malveillants : les logiciels espions qui espionnent les habitudes de l'utilisateur pour lui envoyer de la publicité ciblée. L'affichage de publicité est généralement considéré par le développeur du publiciel comme un moyen de récupérer ses coûts de développement, ce qui permet au développeur d'offrir le logiciel gratuitement ou à faible coût. Les revenus tirés de la publicité permettent ou incitent les développeurs à continuer de développer, maintenir et améliorer le logiciel. Chez CRDF Labs, nous considérons les PUP/Adware comme des logiciels malveillants et nous les bloquons.

Un point important : votre vie privée & Blockulicious

Les utilisateurs de Blockulicious se posent des questions sur le traitement des données que nous faisons avec le produit Blockulicious. Tout d'abord, vous devez noter que tout est décrit dans la fiche du produit et la FAQ de Blockulicious. Blockulicious ne récolte aucune données capable de vous identifier personnellement et même votre ordinateur. Veuillez lire ci-après pour comprendre ce point essentiel :

Dans la fiche du produit, nous insistons sur le fait :

Blockulicious ne se connecte qu'aux serveurs de CRDF Labs pour récupérer la dernière version de la base de données des sites malveillants. Ensuite, tout se passe sur votre navigateur (dans une base de données locale) et nous ne savons pas quels sites internet vous pouvez visiter. Ainsi, vous êtes assuré que de la confidentialité de vos données. Pour CRDF France et ADMINUSLabs, la confidentialité est un enjeu majeur qui ne doit pas être négligé pour entretenir une confiance mutuelle entre nos utilisateurs.

Principe de fonctionnement global

- Afin de pouvoir récupérer la dernière base de données contenant la liste des sites internet malveillants, Blockulicious va se connecter régulièrement sur les serveurs de CRDF (temps réglable directement depuis la configuration de Blockulicious).
- Blockulicious lors d'un blocage va rediriger l'utilisateur vers une page l'informant qu'une adresse internet malveillante a été bloquée par le service. CRDF récupère juste des statistiques sur le

nombre de blocage entraîné sur ce nom de domaine. Rien de plus n'est stocké en base de données, même votre adresse IP n'est pas stockée.

- Lors du téléchargement régulier des mises à jour depuis votre navigateur Web, rien n'est sauvée non plus. Nous sauvegardons juste l'adresse IP de manière temporaire afin de pouvoir calculer des statistiques afin de connaître le nombre d'utilisateurs exact (ceci est amené à disparaître dans les jours à venir [**On parle bien de l'histoire de sauvegarde des adresses IP qui télécharge notre base de données**]).
- Une base de données locale (via du pure JavaScript) permet de détecter les noms de domaine malveillants qui doivent être bloqués par le produit, tout se passe dans votre navigateur. Rien n'est transmis pendant votre navigation aux serveurs de CRDF France.

La vérité est-elle ailleurs ?

Non, elle est bien dans ce billet. Blockulicious est l'un des produits les plus respectueux de votre vie privée puisqu'ils ne transfère aucune données sur votre navigation et nous ne savons pas quelles sites internet vous pouvez visiter.

Des doutes ?

- Le code source de nos extensions est accessible directement depuis la FAQ du produit, vous pouvez même le visualiser directement depuis votre navigateur en mode développeur.
- Analyser les trames réseaux HTTP/HTTPS (TCP) qui passent sur vos installaitons avec Blockulicious d'installé sur votre navigateur et vous ne verrez aucune trame réseau suspecte qui va vers les serveurs de CRDF visant à vous espionner à votre insu.

Avec ceci, vous pourrez vérifier nos dire. Attention : Blockulicious n'est pas un produit OpenSource (le code source est cependant libre à la lecture afin d'analyser le code source), nous distribuons les sources de nos extensions mais elles sont protégées par la propriété intellectuelle de CRDF Labs & CRDF France & Adminus.

Conclusions sur la vie privée & Blockulicious

Blockulicious n'espionne pas vos habitudes de connexion, n'enregistre pas les sites Web que vous visitez et rien ne sort de votre navigateur (tout est en local). CRDF est très clair et précis là-dessus et vous pouvez nous contacter sans aucun problème pour nous poser des questions sur ce produit.

Blockulicious n'est pas un produit Open Source

Blockulicious n'est pas un produit issu du monde du libre mais un système propriétaire appartenant à la société CRDF France (www.crdf.fr) - **Droits de reproduction et de diffusion réservés. International Copyright © 2000 - 2014 CRDF All Rights Reserved.** Cependant, vous devez garder à l'esprit que le code source n'est pas compilé et accessible à tout moment pour démontrer que Blockulicious respecte votre vie privée. De plus, il n'est techniquement pas possible de compiler du code source JavaScript, on pourrait le chiffrer mais cela affecterait considérablement la rapidité de l'extension.

Signaler un lien malveillant au laboratoire CRDF Labs

Si vous pensez qu'un site internet est bloqué par Blockulicious et qu'il ne devrait pas être bloqué, trois solutions s'offrent à vous :

1. Signaler le faux-positif depuis la page de blocage disponible pour chacun des sites internet bloqués (page de redirection qui vous indique que le site a été bloqué).
2. Ouvrir les préférences de l'extension et ajouter le nom de domaine correspondant dans votre liste blanche personnelle.
3. En envoyant un rapport à url@crdf.fr pour nous signaler le faux-positif.

Panneau de configuration (préférences) de Blockulicious

Le panneau de configuration de Blockulicious se présente sous la forme suivante :



Options

Blockulicious - Préférences

Faire un don : [Paypal](#).

☐ Afficher les notifications

☐ Bloquer les publicités

Temps de mise à jour minutes

Dernière mise à jour : 29/8/2014 16:8:36

[Reset de la base de données locale](#) [Mettre à jour](#)

Liste blanche

Pour ajouter un site internet dans vos exceptions et éviter le blocage du dit site internet, vous devez simplement ajouter son nom de domaine sans les 'www.' et les 'http://'.

Exemple : pour débloquent 'http://www.crdf.fr/product/example/', vous devez entrer 'crdf.fr' pour qu'il soit accepté dans votre liste d'exception.

Nous disposons de plusieurs options afin que vous puissiez personnaliser au mieux le produit selon vos besoins.

Préférences de bases

Nous allons expliciter les préférences de bases (de simples cases à cocher). L'option :

1. Afficher les notifications : permet d'afficher une notification à chaque fois que Blockulicious bloque un site internet malicieux contenu dans les bases de données
2. Bloquer les publicités : une fonction capable de bloquer les publicités contenus sur les sites internet (base de données supplémentaire). **Si vous activer/désactiver cette fonctionnalité et pour que les modifications soient prises en compte, merci de bien vouloir cliquer sur le bouton "Reset de la base de données".**

Gestion de la base de données

Blockulicious dispose d'une base de données interne qui est stockée sur votre navigateur (avec localStorage de HTML5/JavaScript). Elle n'est en aucun cas hébergée dans le "Cloud" (= sur Internet). Nous récupérons simplement la base de données à copier localement sur le site internet de CRDF France.

Ainsi, nous avons deux fonctionnalités basiques à retenir dans cette partie :

1. Reset de la base de données : permet d'effacer toute la base de données locale stockée dans votre navigateur et de la synchroniser à nouveau avec les serveurs de CRDF France.
2. Mettre à jour : permet tout simplement de récupérer les dernières définitions des sites internet malicieux en se connectant sur les serveurs de CRDF France.

Corrections d'éventuels problèmes

Il se peut que votre base de données ne soient pas en phase avec celle de CRDF France. Si vous constatez qu'un site internet est bloqué et qu'il n'est plus ou pas contenu dans la base de données des serveurs de CRDF France, vous pouvez effectuer un reset complet de la base de données. Ceci peut, dans la majorité des cas, résoudre votre problème. Si vous rencontrez d'autres difficultés, merci de nous contacter.

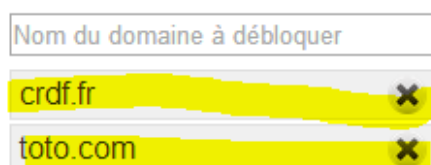
Liste blanche

La liste blanche est une liste d'exception. Elle vous permet de débloquent un site internet malicieux contenu dans les bases de données de CRDF Labs pour que vous puissiez y accéder sans problème. A l'ajout dans la liste blanche, ce nom de domaine sera automatiquement ignoré par l'extension et ne sera plus bloqué par Blockulicious.

Liste blanche

Pour ajouter un site internet dans vos exceptions et éviter le blocage du dit site internet, vous devez simplement ajouter son nom de domaine sans les 'www.' et les 'http://'.

Exemple : pour débloquent 'http://www.crdf.fr/product/example/', vous devez entrer 'crdf.fr' pour qu'il soit accepté dans votre liste d'exception.



La liste des noms de domaine déjà dans votre liste blanche s'affiche en-dessous du champ "Nom du domaine à débloquent". Pour supprimer une entrée de votre liste blanche, veuillez tout simplement cliquer sur la "croix" pour supprimer la dite entrée.

Pour ajouter une entrée dans votre liste blanche, veuillez n'indiquer que le nom de domaine sans les "www." et sans le "http://". Dans le cas contraire, un message vous empêchera de l'ajouter dans la liste blanche puisque le format attendu n'est pas correct.

Plusieurs exemples concrets

1. Débloquer le site internet "http://www.crdf.fr/product/blabla/" revient à mettre dans votre liste blanche "crdf.fr"
2. Débloquer le site internet "http://www.domain.fr/path/blabla/" revient à mettre dans votre liste blanche "domain.fr"
3. Débloquer le site internet "http://google.fr/search" revient à mettre dans votre liste blanche "google.fr"

Et ainsi de suite...

Désinstallation de Blockulicious de votre navigateur

Pour désinstaller Blockulicious de votre navigateur, veuillez consulter la documentation de celui-ci et nous serons triste. Envoyez-nous votre feedback (* vos avis).

A propos de Blockulicious

Aide et support

Si vous avez des questions, des suggestions ou bien un problème avec Blockulicious, nous vous remercions de bien vouloir consulter notre base de connaissance (elle répond à la majorité de vos questions) ou bien contacter l'équipe de développement de l'extension.

Contacts et base de connaissance

[Base de connaissance](#) [Contacter l'équipe en charge du développement de Blockulicious](#)

Conditions générales d'utilisation (en anglais)

Les conditions générales d'utilisation de l'extension (donc de ce produit) sont disponibles à l'adresse suivante :

<http://manager.crdf.fr/knowledgebase.php?action=displayarticle&id=16> > Disponible uniquement en langue anglaise